## ORAL ARGUMENT NOT SCHEDULED No. 23-1032, 23-1073

# IN THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

DAHUA TECHNOLOGY USA INC.

and

HIKVISION USA, INC.,

Petitioners,

v.

FEDERAL COMMUNICATIONS COMMISSION

and

UNITED STATES OF AMERICA,

Respondents.

On Petitions for Review of an Order of the Federal Communications Commission

# BRIEF FOR INTERVENOR MOTOROLA SOLUTIONS, INC. IN SUPPORT OF RESPONDENTS

Thomas M. Johnson, Jr.

Counsel of Record

Bennett L. Ross

Michael J. Showalter

WILEY REIN LLP

2050 M Street NW

Washington, DC 20036

(202) 719-7000

tmjohnson@wiley.law

August 7, 2023

Counsel for Motorola Solutions, Inc.

### CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Cir. Rule 28(a)(1), Intervenor hereby certify as follows:

#### A. Parties and Intervenors:

All parties and intervenors appearing in this Court are listed in the Brief for Petitioners.

**B. Rulings Under Review:** The petitions for review challenge the following order of the Federal Communications Commission: *Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program, Protecting Against National Security Threats to the Communications Supply Chain Through the Competitive Bidding Program, Report and Order, Order, and Further Notice of Proposed Rulemaking, FCC 22-84, ET Docket No 21-232, EA Docket No. 21-233 (rel. Nov. 25, 2022) (the "Order").* 

C. Related Cases: The order under review has not previously been before this Court or any other court. Intervenor is aware of no other related cases within the meaning of D.C. Circuit Rule 28(a)(1)(C).

### **RULE 26.1 DISCLOSURE STATEMENT**

Pursuant to Federal Rule of Appellate Procedure 26.1 and D.C. Cir. Rule 26.1, Intervenor submits the following statement:

Motorola Solutions Inc. ("Motorola") states that it has no parent corporation and that no publicly held company owns 10 percent or more of its stock.

## **TABLE OF CONTENTS**

Page(s)	)
INTRODUCTION	
ISSUES PRESENTED4	
STATUTES AND REGULATIONS	
STATEMENT OF THE CASE	
SUMMARY OF ARGUMENT	
ARGUMENT9	,
I. The Hobbs Act Limitations Period Bars Petitioners' Lead Challenge.	,
A. Petitioners Are Challenging Aspects Of The 2020 Order 10	ı
B. The Hobbs Act Limitations Period Bars Challenge To The 2020 Order	
II. Congress's Ratification Of The FCC's Covered List In The SEA Precludes Petitioners' Lead Challenge	,
III. The FCC Reasonably Interpreted The SNA's Scope	ı
A. The FCC Reasonably Defined Eligible "Essential" Equipment Or Services	
B. The FCC's Decision To Accord Dispositive Weight To Congress's National-Security Determination Was Reasonable	
III. The FCC Reasonably Construed The Scope Of "Critical Infrastructure"	
CONCLUSION 20	

# TABLE OF AUTHORITIES

Page(s)
Cases
Ali v. Fed. Bureau of Prisons, 552 U.S. 214 (2008)30
All. for Safe, Efficient & Competitive Truck Transp. v. FMCSA, 755 F.3d 946 (D.C. Cir. 2014)
Bragdon v. Abbott, 524 U.S. 624 (1998)
Cellco P'ship v. FCC, 357 F.3d 88 (D.C. Cir. 2004)
Commc'ns Vending Corp. of Ariz. v. FCC, 365 F.3d 1064 (D.C. Cir. 2004)
Conn. Nat. Bank v. Germain, 503 U.S. 249 (1992)34
Flat Creek Transp., LLC v. FMCSA, 2017 WL 4172613 (M.D. Ala. 2017)
Forest Grove Sch. Dist. v. T.A., 557 U.S. 230 (2009)19
Functional Music, Inc. v. FCC, 274 F.2d 543 (D.C. Cir. 1958)
Garcia v. United States, 469 U.S. 70 (1984)29, 30
Gorss Motels, Inc. v. FCC, 20 F.4th 87 (2d Cir. 2021)
*Harrison v. PPG Indus., Inc., 446 U.S. 578 (1980)
*Authorities upon which we chiefly rely are marked with asterisks.

<i>Hire Ord. Ltd. v. Marianos</i> , 698 F.3d 168 (4th Cir. 2012)	15
*Huawei Techs. USA, Inc. v. FCC, 2 F.4th 421 (5th Cir. 2021)	38, 39
JEM Broad. Co. v. FCC, 22 F.3d 320 (D.C. Cir. 1994)	16
Kokkonen v. Guardian Life Ins. Co. of Am., 511 U.S. 375 (1994)	14
*Krause v. Titleserv, Inc., 402 F.3d 119 (2d Cir. 2005)	22, 23
Lamie v. U.S. Tr., 540 U.S. 526 (2004)	34
Lewis v. City of Chicago, 560 U.S. 205 (2010)	28
Morrison–Knudsen Constr. Co. v. DOL, 461 U.S. 624 (1983)	31
Motorola Sols., Inc. v. Hytera Commc'ns Corp., No. 1:17-cv-1973, 2021 WL 3076780 (N.D. Ill. Mar. 10, 2021)	35
<i>Mozilla Corp. v. FCC</i> , 940 F.3d 1 (D.C. Cir. 2019)	25
*Nat'l Lifeline Ass'n v. FCC, 983 F.3d 498 (D.C. Cir. 2020)	12, 15
Nat'l Min. Ass'n v. DOI, 70 F.3d 1345 (D.C. Cir. 1995)	13
Nielson v. Preap, 139 S.Ct. 954 (2019)	33
NLRB Union v. FLRA, 834 F.2d 191 (D.C. Cir. 1987)	15

Oljato Chapter of Navajo Tribe v. Train, 515 F.2d 654 (D.C. Cir. 1975)	14
Overdevest Nurseries, L.P. v. Walsh, 2 F.4th 977 (D.C. Cir. 2021)	29
PDR Network, LLC v. Carlton & Harris Chiropractic, Inc., 139 S. Ct. 2051 (2019)	12
Polselli v. IRS, 143 S. Ct. 1231 (2023)	33
Pub. Emps. for Env't Resp. v. EPA, 2023 WL 4714021 (D.C. Cir. 2023)	13
Return Mail, Inc. v. United States Postal Serv., 139 S. Ct. 1853 (2019)	31, 32
Sossamon v. Texas, 563 U.S. 277 (2011)	14
<i>Texas v. United States</i> , 730 F.2d 409 (5th Cir. 1984)	23
<i>United States v. Stevens</i> , 691 F.3d 620 (5th Cir. 2012)	16
United States v. Turkette, 452 U.S. 576 (1981)	30
*United Transp. Union-Ill. Legislative Bd. v. Surface Transp. Bd., 132 F.3d 71 (D.C. Cir. 1998)	
Vernal Enters., Inc. v. FCC, 355 F.3d 650 (D.C. Cir. 2004)	11
Water Transp. Ass 'n v. ICC, 722 F.2d 1025 (2d Cir. 1983)	23
Weaver v. FMCSA, 744 F.3d 142 (D.C. Cir. 2014)	14, 15

### **Statutes**

20 U.S.C. § 1098bb(a)(1)33
28 U.S.C. § 2342(1)9
47 U.S.C. § 1601(b)(2)28, 29, 30, 31, 33
47 U.S.C. § 1608(4)21, 23
47 U.S.C. § 1302(d)(1)21
47 U.S.C. § 1601(b)
47 U.S.C. § 1601(b)(1)32, 33
47 U.S.C. § 1601(b)(2)(A)
47 U.S.C. § 1601(b)(2)(C),
47 U.S.C. § 1601(c)
47 U.S.C. § 1601(c)(3)24, 27
47 U.S.C. § 1601 note
47 U.S.C. § 1602
47 U.S.C. § 1602(b)(2)28
47 U.S.C. § 1602(b)(2)(C)28
47 U.S.C. § 1603
47 U.S.C. § 1608(1)21
John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, §889, 132 Stat. 1636 3, 4, 7, 8, 17, 21, 24, 25, 26, 27, 28, 34
Secure and Trusted Communications Networks Act of 2019, Pub. L. 116-124, 134 Stat. 158

Secure Equipment Act of 2021, Pub. L. No. 117-55, § 2(a)(2), 135 Stat. 423	5, 7, 17, 18
28 U.S.C. § 2344	9
Other Authorities	
164 Cong. Rec. S3,285-02 (daily ed. June 7, 2018)	26
164 Cong. Rec. S5,541-01 (daily ed. Aug. 1, 2018)	26
85 Fed. Reg. 230-01, 2020 WL 30573 (Jan. 3, 2020)	35
Antonin Scalia & Bryan A. Garner, Reading Law (2012).	29, 32
Brett M. Kavanaugh, <i>Fixing Statutory Interpretation</i> , 129 Harv. L. Rev. 2118 (2016)	30
Oxford Eng. Dictionary	23
Black's Law Dictionary (11th ed. 2019)	23
Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program, ET Docket No. 21-232, Notice of Proposed Rulemaking, FCC 21-73, ¶ 15 (June 17, 2021)	10
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program, Notice of Proposed Rulemaking and Notice of Inquiry, 36 FCC Rcd. 10578 (2021)	18
Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program, Protecting Against National Security Threats to the Communications Supply Chain Through the Competitive Bidding Program, Report and Order, Order and Further Notice of Proposed Rulemaking, FCC 22-84, ET Docket No. 21-232, EA Docket No. 21-233 (rel. Nov. 25, 2022)	, 37, 38, 39

Protecting Against National Security Threats to the Communic Supply Chain Through FCC Programs, Report and Order, Further Notice of Proposed Rulemaking Order, 34 FCC Rcd. 11423 (2019)	and
Protecting Against National Security Threats to the Communic	cations
Supply Chain Through FCC Programs,	
WC Docket. No. 18-89, Second Report and Order, 35 FCC	Rcd
14284 (2020)	17, 18, 20, 21, 25, 35

# **GLOSSARY**

APA	Administrative Procedure Act
Covered List	Covered List of communications equipment produced by foreign companies in the 2019 Secure and Trusted Communications Networks Act
FCC or Commission	Federal Communications Commission
Petitioners	Hikvision USA, Inc. and Dahua Technology USA, Inc.
SNA	2019 Secure and Trusted Communications Networks Act
SEA	2021 Secure Equipment Act
Section 889	Section 889 of the 2019 National Defense Authorization Act
Section 1601	47 U.S.C. § 1601

#### INTRODUCTION

Congress and the Federal Communications Commission have placed Petitioners' video-surveillance equipment that meets certain criteria on the Covered List for one simple reason—it endangers national security. In a series of statutes and orders, the federal government has with one voice determined that this equipment should not connect with government networks, should not be subsidized with federal dollars, and—in the Order under review—should not be authorized for use in connection with American broadband networks. This case does not require this Court to guess at Congress's intent or speculate on the scope of the Commission's authority. In the Secure Equipment Act ("SEA"), Congress expressly directed the Commission to "clarify that the Commission will no longer review or approve any application for equipment authorization for equipment that is on the list of covered communications equipment or services published by the Commission," 47 U.S.C. § 1601 note—which includes Petitioners' equipment.

Motorola Solutions, Inc. ("Motorola"), a global leader in mission-critical communications that deploys and advances the communications networks the Order is designed to protect, supports the Order consistent with its longstanding commitment to ensuring the highest level of security for public safety, law enforcement, critical infrastructure, and governmental networks. As Motorola knows all too well, and Congress has explicitly concluded, companies that produce

equipment on the Covered List pose a significant national-security risk. One covered equipment producer stole Motorola's intellectual property, engaging in conduct so egregious that it resulted in a multi-hundred-million dollar civil-jury verdict against the producer as well as a criminal indictment of the producer and several of its employees, along with severe, ongoing irreparable harm.

Petitioners' challenges to the Order are baseless. The Court should not even reach the merits of Petitioners' lead arguments because they are untimely. Petitioners bring this action under the Hobbs Act, which has a sixty-day limitations period. Yet their lead challenge—as they acknowledge—is to the FCC's inclusion of their equipment on the Covered List in a 2020 order. The 2023 Order merely builds upon that 2020 order as Congress required and does not reopen the 2020 order to challenge.

Petitioners' arguments fail on the merits too because the Order is amply supported by statute. In fact, Congress in the SEA ratified and endorsed the very FCC actions Petitioners challenge, including the placement of their equipment on the Covered List. The Order is merely the latest step in an iterative collaboration between Congress and the Executive Branch, and when the political branches are operating as designed, the judiciary should not interfere.

The FCC, moreover, reasonably construed the scope of the pertinent statutory terms. The Secure Networks Act ("SNA") requires the FCC to place certain

"communications equipment or service" on the Covered List and defines that phrase as "any equipment or service that is essential to the provision of advanced communications service," which includes "video telecommunications using any technology." The FCC reasonably determined that this phrase encompasses all equipment used in fixed and mobile broadband networks that uses electronic components. Petitioners read "essential" to mean "absolutely indispensable," but courts have cautioned that "essential" should not be read so inflexibly, and the FCC's less restrictive approach is owed deference. Indeed, Congress itself has left no doubt that its understanding of the word aligns with that of the FCC. And Petitioners' preferred definition would neuter the statute because it is unlikely that *any* equipment is literally indispensable to a network's operation given the redundancies built into modern networks.

The FCC's determination that Petitioners' equipment poses unacceptable national-security risk because Congress determined that it does also is reasonable, and Petitioners' contrary argument is premised on a rewrite of the plain statutory text. The SNA provides that the FCC must place equipment on the Covered List when one of four enumerated determinations is made and the equipment is "capable of" posing an unacceptable national-security risk. It is undisputed that the enumerated-determination prong is satisfied because Congress determined in the National Defense Authorization Act ("NDAA") that Petitioners' equipment poses

an unacceptable national-security risk. Petitioners nevertheless assert that their equipment is not "capable of" posing an unacceptable national-security risk because the statute (in their view) requires that the national-security risk relate to a device's ability to interact harmfully with a network. But the statutory text contains no such limitation, and this Court should apply the text as written.

Finally, the FCC reasonably construed the scope of the NDAA term "critical infrastructure." Petitioners assert that the Order makes all infrastructure critical, including "used car lots," but that is a gross mischaracterization. The Order simply borrows from elsewhere in federal law in describing what facilities "could" be deemed critical infrastructure. The Order takes no position on whether any particular facility constitutes critical infrastructure; rather, it establishes a process under which Petitioners and others can obtain approval for their equipment so long as it will not be used for an improper purpose. Petitioners' challenge, therefore, is both premature and meritless.

For all these reasons, the petitions for review should be dismissed.

#### **ISSUES PRESENTED**

1. Whether the Hobbs Act's sixty-day limitations period bars Petitioners' challenges to aspects of an FCC order from 2020.

- 2. Whether Congress's endorsement of the FCC's Covered List in the SEA precludes Petitioners' challenge to the inclusion of their equipment on the Covered List.
- 3. Whether the Commission reasonably construed the term "essential" in the SNA.
- 4. Whether the Commission reasonably relied on Congress's determination that Petitioners' equipment poses unacceptable national-security risk when placing Petitioners' equipment on the Covered List.
- 5. Whether the Commission reasonably construed the scope of "critical infrastructure" in providing guidance for what kinds of equipment may be placed on the Covered List.

#### STATUTES AND REGULATIONS

Pertinent statutes and regulations are contained in an addendum to the Respondent brief.

#### STATEMENT OF THE CASE

Motorola adopts the Respondent brief's Statement of the Case.

#### **SUMMARY OF ARGUMENT**

I. Most of this petition is untimely. Petitioners do not hide the ball—their main argument is that their equipment "does not belong on the Covered List." Pet. Br. 2.

Because the FCC placed their equipment on the Covered List in 2020, the Hobbs Act's sixty-day limitations period bars that argument.

A. Petitioners do not dispute that the FCC placed their equipment on the Covered List in a 2020 order. Nor do they dispute that this 2020 order adopted the construction of "essential" that they now seek to challenge. And they do not deny that the 2020 order rejected the notion that the FCC must in all circumstances independently assess a piece of equipment's capacity to threaten national security. Yet those 2020 decisions make up almost the entirety of what Petitioners now challenge.

**B.** The Hobbs Act limitations period—which is jurisdictional—bars Petitioners' attacks on the inclusion of their equipment on the Covered List. The Hobbs Act exists to ensure the swift resolution of any uncertainty surrounding the lawfulness of agency rules—it channels facial challenges to a single court and produces a single ruling on all potential facial challenges. If every new order exposed to legal challenge all prior orders it presupposes, Hobbs Act finality could not exist. Here, this Court's reopening exception does not apply because the FCC did not reconsider the 2020 order. And the *Functional Music* exception does not apply either, because it allows only as-applied challenges to party-specific administrative actions, not facial attacks on industry-wide rulemakings.

**III.** The FCC reasonably interpreted the scope of the SNA, and Petitioners' arguments to the contrary contradict the statutory text.

A. The FCC's interpretation of "essential" under the SNA was reasonable. Courts should exercise appropriate deference to an agency's elucidation of such an "open-textured" term. *Huawei*, 2 F.4th at 437. Petitioners' interpretation of "essential" as "absolutely indispensable," moreover, is not the best reading. Numerous courts have cautioned against reading "essential" so inflexibly. And here, Congress itself expressed its intent in the SNA to cover video-surveillance equipment, as evidenced by the statute's reference to Section 889(f)(3) of the NDAA. *See* Order 7608. Furthermore, Petitioners' definition would neuter the statute since virtually *no* equipment is absolutely indispensable to modern broadband

networks. Petitioners offer no limiting principle for their maximally restrictive definition.

**B.** It was reasonable for the FCC to accord dispositive weight to Congress's determination that Petitioners' equipment poses a national-security risk. Section 1601(b) of the SNA requires the FCC to place equipment on the Covered List when one of four enumerated national-security determinations is made by specified federal entities and the equipment is "capable of" posing unacceptable national-security risks. Petitioners' argument that their equipment is not capable of posing unacceptable national-security risk under that second prong—despite Congress's determination in the NDAA that their equipment does in fact pose unacceptable national-security risks—contradicts the plain statutory text. Petitioners invoke the noscitur and ejusdem canons to ask the Court to read into the text a requirement that equipment "capable of" unacceptable risk must specifically pose a risk of networkinteraction harm, but those canons do not apply here and cannot trump the plain text in any event. Petitioners concede, moreover, that their interpretation violates the canon of consistent usage. The FCC's determination that equipment that Congress deems threatening to national security does in fact threaten national security is consistent with the statutory text and eminently reasonable.

**IV.** Finally, the FCC reasonably construed the scope of "critical infrastructure." The FCC simply stated that it would construe the term consistently

with how it is used elsewhere in federal law and that certain facilities "could" be deemed critical infrastructure under that understanding. The Commission did not apply the term to specific facilities but rather established parameters for what critical infrastructure is and stated that further determinations about specific pieces of equipment will be forthcoming after consultation from responsible executive branch agencies. Petitioners' challenge is both premature and meritless.

#### **ARGUMENT**

#### I. The Hobbs Act Limitations Period Bars Petitioners' Lead Challenge.

This case arises under the Hobbs Act, see Pet. Br. 5 (citing 28 U.S.C. § 2342(1)), which carries a sixty-day limitations period, but Petitioners' lead arguments challenge an order entered three years ago. Specifically, the arguments advanced in Argument Sections I and II of Petitioners' brief are barred because they challenge the 2020 order that included their video equipment on the Covered List.

The Hobbs Act gives federal courts of appeals exclusive jurisdiction to review "all final orders of the [FCC] made reviewable by section 402(a) of title 47." 28 U.S.C. § 2342(1). And the Act provides that a person aggrieved by a final order reviewable under the Act may file a petition for review "within 60 days after [the order's] entry." Id. § 2344. That limitations period "is jurisdictional in nature, and may not be enlarged or altered by the courts." All. for Safe, Efficient & Competitive Truck Transp. v. FMCSA, 755 F.3d 946, 950 (D.C. Cir. 2014).

### A. Petitioners Are Challenging Aspects Of The 2020 Order.

The agency action Petitioners primarily challenge became final years ago. As evident from the first sentence of their Summary of Argument, Petitioners' lead challenge is that "the Commission erred by subjecting Petitioners' video equipment to the Covered List." Pet. Br. 19; see also id. at 2 ("Petitioners' video equipment ... does not belong on the Covered List."). And the Commission subjected Petitioners' video equipment to the Covered List in 2020. See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, WC Docket No. 18-89, Second Report and Order, 35 FCC Red 14284 (2020) (the "2020 order"). Indeed, in comments to the FCC, Hikvision candidly acknowledged that it "challenge[s] ... the rule" "placing Hikvision on the Covered List," i.e., the 2020 order. Hikvision Apr. 7, 2022 Letter to FCC at 2.

Petitioners do not contest that the 2020 order made clear that the FCC "will incorporate onto the Covered List [certain] equipment from ... Hikvision ... and Dahua" and then explicitly mandated that such equipment be incorporated. 2020 order ¶¶ 68–69; see also Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program, ET Docket No. 21-232, Notice of Proposed Rulemaking, FCC 21-73, ¶ 15 (June 17, 2021) ("A core component of [the 2020 order] concerns the creation and publication of the Covered List."). And as Petitioners explain, the FCC ultimately "announced"

a List including Petitioners' [v]ideo surveillance and telecommunications equipment" "[i]n March 2021." Pet. Br. 14 (cleaned up).

Furthermore, Petitioners acknowledge that it is "the [2020] Supply Chain Second Report and Order" that "adopted [the] construction of the statutory term 'essential to." Id. at 13 (cleaned up). And in the 2020 order the Commission also considered and rejected the notion that in all circumstances it must independently consider a piece of equipment's capability to threaten national security. See 2020 order ¶¶ 79–83. These are precisely the conclusions that Petitioners now belatedly challenge. Pet. Br. 24–40.

# B. The Hobbs Act Limitations Period Bars Challenge To The 2020 Order.

Petitioners' attacks on the 2020 order "must be dismissed." Vernal Enters., Inc. v. FCC, 355 F.3d 650, 655 (D.C. Cir. 2004) (Hobbs Act petition was not filed within 60 days). Petitioners have never contested that the 2020 order is a "final order" covered by the Hobbs Act. And Petitioners did not challenge the order within 60 days. Nor did anyone else. The FCC's inclusion of Petitioners' equipment on the Covered List, therefore, cannot be challenged in this litigation.

Allowing Petitioners to challenge the 2020 order would undermine Hobbs Act finality and the reasons it exists. The "point of the Hobbs Act" is to "force parties who want to challenge agency orders via facial, pre-enforcement challenges to do so promptly," which ensures the swift resolution of any "uncertainty" surrounding the

USCA Case #23-1032

lawfulness of agency rules. PDR Network, LLC v. Carlton & Harris Chiropractic, Inc., 139 S. Ct. 2051, 2059 (2019) (Kavanaugh, J., concurring in the judgment). In conjunction with the exclusive-jurisdiction provision, the limitations period serves as a "channeling device" under which the court selected to hear an initial facial challenge produces a "ruling on all of the facial challenges that could ever arise." Gorss Motels, Inc. v. FCC, 20 F.4th 87, 96 (2d Cir. 2021). That "alleviates the confusion that would ensue from conflicting rulings, dueling stays, and incongruent appeals." Id. But if every new rulemaking exposed to challenge all prior rules presupposed by the new rule, Hobbs Act finality would be defeated every time the agency amends or supplements its existing rules. See, e.g., Nat'l Lifeline Ass'n v. FCC, 983 F.3d 498, 509 (D.C. Cir. 2020) (new declaratory ruling concerning the FCC Lifeline program did not open door to a challenge to the "legality of any existing rule covering the Lifeline program").

Petitioners' counterarguments only underscore the point. In comments to the FCC, Hikvision argued that it may challenge the 2020 order because the 2023 Order "expands the [2020 order] to reach equipment authorizations." Hikvision Apr. 7, 2022 Letter to FCC at 2. Hikvision asserted that this expansion of the 2020 order allows it to challenge "both the new application and the underlying rule." Id. at 3. That is wrong. No doubt, Petitioners may challenge any new decisions made in the 2023 Order even though they build on the 2020 order's foundation. But allowing Petitioners to challenge decisions made in the 2020 order itself "would make a mockery of Congress' careful effort to force potential litigants to bring challenges to a rule issued under this statute at the outset." *Nat'l Min. Ass'n v. DOI*, 70 F.3d

Filed: 08/07/2023

Order are reviewable.

Although Petitioners "[have] not mention[ed] it," their position "relies on the reopening doctrine," which "allows an otherwise stale challenge to proceed because 'the agency opened the issue up anew,' and then 'reexamined ... and reaffirmed its [prior] decision." All. for Safe, Efficient & Competitive Truck Transp., 755 F.3d at 950, 953. But that doctrine "only applies" when "the agency has undertaken a serious, substantive reconsideration of the existing rule." *Id.* at 954; see also Pub. Emps. for Env't Resp. v. EPA, 2023 WL 4714021, at \*10 (D.C. Cir. 2023) (petitioner has "burden to show the agency's 'clear' intent to reopen the administrative proceeding"). Petitioners have not advanced an argument that the FCC reconsidered the 2020 order, and it did not. At most, in responding to Petitioners' arguments, the FCC reiterated the conclusions made in the prior order and built upon that established foundation. And that does not constitute reopening. "An agency does not 'reopen' an issue ... when in response to comments that are beyond the scope of the rulemaking it merely reaffirms its prior position." United Transp. Union-Ill. Legislative Bd. v. Surface Transp. Bd., 132 F.3d 71, 76 (D.C. Cir. 1998). That is

1345, 1351 (D.C. Cir. 1995). Only decisions announced for the first time in the 2023

because the reopening doctrine "is not a license for bootstrap procedures by which petitioners can comment on matters other than those actually at issue, goad an agency into a reply, and then sue on the grounds that the agency had re-opened the issue." *Id*.

Nor does the Functional Music exception to Hobbs Act finality apply. The exception is a narrow one. See, e.g., Kokkonen v. Guardian Life Ins. Co. of Am., 511 U.S. 375, 377 (1994) (the law "presume[s]" that "a cause lies outside [the federal courts'] limited jurisdiction"); Sossamon v. Texas, 563 U.S. 277, 292 (2011) (waiver of sovereign immunity "must be 'strictly construed""). As cases Hikvision cited to the agency demonstrate, while the exception allows as-applied challenges in certain circumstances, it prohibits facial challenges. E.g., Weaver v. FMCSA, 744 F.3d 142, 145 (D.C. Cir. 2014) (when an agency "seeks to apply [a] rule, those affected may challenge that application," but "facial challenges to [a] rule ... are barred" under the Hobbs Act (citing Functional Music, Inc. v. FCC, 274 F.2d 543, 546 (D.C. Cir. 1958))). That is, "cases like Functional Music" "allow a limited exception to a statutory time limit" "where a party may challenge a specific application of an invalid rule" but do not allow a "general out-of-time challenge to the validity of an [agency] standard," which is "exactly what Congress intended to bar." Oljato Chapter of Navajo Tribe v. Train, 515 F.2d 654, 660 (D.C. Cir. 1975). In a recent case, accordingly, this Court noted that while the petitioner was challenging a new

declaratory ruling concerning an established agency program, "any ... challenge" to "the legality of [an] existing rule covering the [] program" "would likely be untimely." *Nat'l Lifeline Ass'n*, 983 F.3d at 509.

The distinction between facial and as-applied assertions explains why the Functional Music exception applies paradigmatically in a "defense in an enforcement proceeding" or "an appeal from an agency's refusal to reconsider its denial of a petition for rescission of the disputed regulations." NLRB Union v. FLRA, 834 F.2d 191, 195, 196 n.6 (D.C. Cir. 1987); see also id. (Functional Music "itself involved" the latter category); Hire Ord. Ltd. v. Marianos, 698 F.3d 168, 170 (4th Cir. 2012) (Functional Music did not "involve a facial challenge"). Functional Music cases involve party-specific administrative actions taken pursuant to a previously adopted rule. In Weaver, for example, the new agency action was not a "rule[] or regulation[]," and the claim "did not necessarily require the court to consider the validity of [the agency's] use of [its general] system or other rules or regulations subject to the Hobbs Act." Flat Creek Transp., LLC v. FMCSA, 2017 WL 4172613, at \*9 (M.D. Ala. 2017). Rather, the plaintiff asserted in district court that the agency failed to satisfy statutory duties to "ensure" that "data is complete, timely, and accurate," and "provide for review and correction" of inaccurate data, as applied to the plaintiff. Weaver, 744 F.3d at 143 (citing relevant provisions). The FCC proceeding here, on the other hand, involves a new industry-wide rule that

USCA Case #23-1032

simply incorporates by reference the FCC's preexisting final rule establishing the Covered List.

Hikvision argued to the FCC that it "had no reason" to challenge the inclusion of its equipment on the Covered List, Hikvision Apr. 7, 2022 Letter to FCC at 4, but that is not plausible and is irrelevant even if true. It is implausible because the Covered List is a list of equipment that "pose[s] an unacceptable risk to the national security." 2020 order ¶ 1. Surely Petitioners "had ... reason" to object to the inclusion of their equipment on a list of that significance if they believed their equipment did not belong there. And Hikvision's argument is irrelevant in any event because the 2020 order "was subject to immediate challenge" by those companies adversely affected by it, and it would be "of no moment" even if "[Hikvision], in particular, had no opportunity to challenge [certain] rules" within the limitations period. JEM Broad. Co. v. FCC, 22 F.3d 320, 326 (D.C. Cir. 1994). That is because "[s]trict enforcement of [a statutory] time limit is necessary to preserve finality in agency decisionmaking" and justified by "the value of repose." Id. Companies may have myriad reasons not to spend the time and resources to challenge a specific rule, but that cannot undermine Congress's interest in facial finality.

By trying "to raise [facial] challenges much later than they would have been required to had they followed the proper channels," Petitioners attempt an improper "end run" around the Hobbs Act's limitations period. *United States v. Stevens*, 691

their challenges to the 2020 order.

# II. Congress's Ratification Of The FCC's Covered List In The SEA Precludes Petitioners' Lead Challenge.

Even if timely, Petitioners' argument that their equipment should not be included on the Covered List is foreclosed by Congress's decision in the SEA to ratify their inclusion. The SEA is the latest enactment in an iterative process in which Congress has endorsed and expanded upon the Commission's orders in the national-security space. And in the SEA, Congress specifically endorsed the Commission's decision to include Petitioners' equipment on the Covered List.<sup>1</sup>

As Petitioners cannot help but explain, the Covered List is a product of years-long efforts by Congress and the Executive Branch to protect against national-security risks. In Section 889 of the NDAA, adopted in 2018, Congress prohibited the federal government from using or procuring certain telecommunications and video-surveillance equipment. Pub. L. No. 115–232 § 889; *see also* Pet. Br. 9–10. In November 2019, the FCC issued the *Supply Chain First Report and Order*, which drew on Section 889 in establishing a process to prevent subsidies from flowing to companies using certain equipment that poses a national-security threat. *Protecting* 

\_

<sup>&</sup>lt;sup>1</sup> Because the SEA provides clear authority for the Commission to adopt the Order, this Court need not reach the question of whether the agency's Title III authority independently supports the Order.

Against National Security Threats to the Communications Supply Chain Through FCC Programs, Report and Order, Further Notice of Proposed Rulemaking and Order, 34 FCC Rcd. 11423 (2019); see also Pet. Br. 10. Then in March 2020, Congress enacted the SNA, which required the FCC to create the Covered List, provided that equipment on the Covered List is not eligible for FCC subsidies, and made removal and replacement costs (rip and replace) eligible for reimbursement by the FCC. See 47 U.S.C. §§ 1602, 1603; Pet. Br. 11–12.

The FCC began implementing the SNA with its 2020 order, and—most relevant here—decided that it "will incorporate onto the Covered List [certain] equipment from ... Hikvision ... and Dahua." 2020 order, ¶¶ 68–69; see also Pet. Br. 14. Then in June 2021, the FCC proposed the rules at issue here to prohibit all equipment on the Covered List from receiving equipment authorization. Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program, Notice of Proposed Rulemaking and Notice of Inquiry, 36 FCC Rcd. 10578 (2021); see also Pet. Br. 15.

With that backdrop, in November 2021 Congress passed the SEA, endorsing the FCC's actions and directing "the Commission to clarify in [its] pending rulemaking that the Commission would no longer review or approve any applications for equipment authorization for equipment that is on the Covered List." Pet. Br. 15 (cleaned up) (citing Secure Equipment Act of 2021, Pub. L. No. 117-55,

§ 2(a)(2), 135 Stat. 423, 423); *see also* Order 7595 (Congress "specifi[ed] ... this proceeding, by its docket number."). Similarly, Congress also endorsed "the [FCC's] definition of covered equipment and services" for the rip-and-replace program by incorporating it in an amendment to the SNA. *Huawei*, 2 F.4th at 432 (citing Pub. L. No. 116-260, 134 Stat. 1182, 2120 (Dec. 27, 2020)).

As Petitioners acknowledge, their video equipment was on the Covered List when Congress "direct[ed]" the FCC to "no longer review or approve" any equipment-authorization application for any equipment "on the Covered List." Pet. Br. 15 (cleaned up); see also Forest Grove Sch. Dist. v. T.A., 557 U.S. 230, 239 (2009) ("Congress is presumed to be aware of an administrative ... interpretation of a statute."). And as Petitioners further acknowledge (at 16), "[t]he challenged Order implements this directive" from Congress. Petitioners' argument (at 19) that "the Commission erred by subjecting Petitioners' video equipment to the Covered List" is therefore foreclosed by Congress's "affirmative ratification of the administrative interpretations," Bragdon v. Abbott, 524 U.S. 624, 645-46 (1998)—and instruction to the Commission to continue to accord those interpretations legal effect.

In a similar context, the Fifth Circuit recognized that Congress, following the FCC's adoption of a rule implementing the SNA, "show[ed] [its] approval of the FCC's assertion of authority in the rule" by providing for reimbursement to Universal Service Fund recipients whose networks included rip-and-replace

equipment designated by the Commission. *Huawei*, 2 F.4th at 445. The same reasoning applies here. Congress was aware that the FCC had published a Covered List, and without expressing any disapproval of the agency's actions, made that Covered List the basis for the scope of its instruction to the Commission to ban future equipment authorizations. As the FCC noted, the Order simply "builds upon ongoing efforts by Congress, the Executive Branch, and the Commission to protect our nation's networks and supply chains." Order 7594; *see also id.* ("The Commission's actions in this proceeding fulfill Congress's mandate that the Commission adopt such rules."). In other words, the Order is simply the natural next step in the FCC's process for implementing Congress's enacted will. It must be sustained for that reason alone.

### III. The FCC Reasonably Interpreted The SNA's Scope.

Because Petitioners' challenges are untimely, and because in any event Congress ratified the 2020 order, this Court should not reach the merits of Petitioners' challenges to the scope of the FCC's authority under the SNA. But in any event, the FCC's interpretations of the SNA were entirely permissible.

Petitioners' challenge to the FCC's interpretations rests on strained and atextual readings of the statute. As Dahua previously recognized, "the Commission had no choice but to publish the Covered List and to include certain categories of Dahua equipment on that list as a result of Congress' determination to designate

certain Dahua equipment as 'covered' in Section 889(f)(3)." Dahua Apr. 7, 2022 Letter to FCC at 3; see also id. ("[T]he Commission does not have discretion to disregard" "Congress's decision to identify [Dahua's] products as 'covered equipment."). Dahua now argues the opposite, but it was right the first time—Section 1601 required the FCC to place Petitioners' equipment on the Covered List.

# A. The FCC Reasonably Defined Eligible "Essential" Equipment Or Services.

The SNA provides that the FCC shall place certain "communications equipment or service" on the Covered List. 47 U.S.C. §§ 1601(b), (c). The Act defines "communications equipment or service" as "any equipment or service that is essential to the provision of" (as relevant here) "video telecommunications using any technology." *Id.* §§ 1608(1), (4); § 1302(d)(1). The FCC reasonably determined that "communications equipment or service" encompasses "all equipment or services used in fixed and mobile broadband networks, provided they include or use electronic components." 2020 order ¶ 52. As the FCC observes (at 45), "[P]etitioners' video cameras and recorders are ... essential to ... the transmission of video information over the internet for video surveillance."

Petitioners argue (at 28) that this determination is impermissible because in their view "equipment is 'communications equipment' only if it is indispensable to the provision of broadband service," but the FCC rightly rejected that cramped interpretation. As an initial matter, when Congress uses "an open-textured term,"

courts should give appropriate weight to an agency's elucidation of that term. *Huawei*, 2 F.4th at 437; *see also Cellco P'ship v. FCC*, 357 F.3d 88, 93–94 (D.C. Cir. 2004) (rejecting petitioners' "attempt ... to elicit from this court a narrow interpretation of [a statutory] word" in part because under "highly deferential" arbitrary-and-capricious review the court "presumes the validity of agency action"); *Commc'ns Vending Corp. of Ariz. v. FCC*, 365 F.3d 1064, 1073 (D.C. Cir. 2004) ("Because Congress did not define the [statutory term], we must determine whether the agency's interpretation is 'based on a permissible construction of the statute.""). The FCC's interpretation here was reasoned and reasonable.

Petitioners suggest (at 28–29) that the term "essential" must in all contexts mean "[a]bsolutely necessary" and "indispensabl[e]," but courts have rightly rejected that sweeping assertion. The Second Circuit, for example, has recognized that while "essential" *can* mean indispensable in certain contexts, "[i]n use, its meaning varies considerably from one context to another." *Krause v. Titleserv, Inc.*, 402 F.3d 119 (2d Cir. 2005). When one says "it is 'essential' when driving a car to stay alert," for example, that "does not mean it is impossible to drive a car without being alert." *Id.* An "essential' question," similarly, is not one that "had to be asked" but one that "goes to the heart of the matter." *Id.* Like its synonym "necessary," the word "essential" is "ambiguous," "[p]articularly as used in the law." *Id.* Those words do not "ha[ve] inflexible meaning" but rather are "used in a sense more or less strict,

Filed: 08/07/2023 Page 34 of 53

according to the subject." *Id.* (quoting M'Culloch v. Maryland, 17 U.S. (4 Wheat.) 316, 388 (1819)); see also, e.g., Water Transp. Ass'n v. ICC, 722 F.2d 1025, 1031 (2d Cir. 1983) ("What is 'essential' depends upon the purposes to be served and those purposes may vary widely from legal context to legal context."); Texas v. United States, 730 F.2d 409, 417 (5th Cir. 1984) ("What is essential must be determined in the light of the structure and purpose of the [statute]."). Even if Section 1608(4)'s "essential" is read in the word's "necessary" sense, therefore, Petitioners' "absolutely indispensable" gloss does not follow.

Moreover, Petitioners' own sources list senses of essential that are not about necessity—such as "[o]f, relating to, or involving the essence or intrinsic nature of something," Essential, Black's Law Dictionary (11th ed. 2019) (definition 1), or "[t]hat is such by essence," Essential, adj. and n., Oxford Eng. Dictionary, http://www.oed.com/view/Entry/64503 (last visited June 1, 2023) (definition 1.a); see also id. (definition 1.d: "[d]ependent on the intrinsic character or condition of anything..."). The Commission's decision to include "all equipment or services used in fixed and mobile broadband networks" fits comfortably within this meaning of "essential"—equipment which, by its essence or nature, is used in the provision of video surveillance or other advanced communications services.

Importantly, Congress itself elected not to limit the scope of covered "communications equipment or service" to equipment "absolutely necessary" for

covered services. Section 889(f)(3) expressly defines "covered telecommunications" equipment or services" as including "video surveillance and telecommunications equipment produced by ... Hikvision Digital Technology Company ... or Dahua Technology Company." Pub. L. No. 115–232 § 889(f)(3). And the SNA makes clear that this Section 889(f)(3) term is a subset of the SNA term "communications equipment or service." 47 U.S.C. § 1601(c)(3). While Petitioners cite Section 889(f) to argue (at 30) that communications equipment or services cannot include videosurveillance equipment, therefore, Section 889(f)(3) states that it does.

Furthermore, Petitioners' interpretation—that "essential" must be read as "absolutely necessary" and "indispensable," Pet. Br. 28—would neuter the statute. In their effort to carve out their equipment from the "essential" definition, Petitioners have offered a definition that would exclude core network equipment as well. Modern broadband networks involve thousands of interconnected cables, towers, wireless facilities, and other devices and components deployed on a regional, national, or even global basis. These networks typically build in redundancies to ensure sufficient capacity to prevent interruption in service or diminution in quality. Given this reality, it is difficult to imagine what, if any, equipment would qualify as literally indispensable to a network's operation. And Petitioners offer no limiting principle whatsoever. An agency has no obligation to adopt an absurd interpretation that would undermine Congress's stated purpose to protect network security. Rather,

it was much more natural—and at minimum, was permissible—for the agency to interpret "essential" to mean equipment that, by its nature, can be used in or connected to a broadband network, and thus would be vulnerable to attack.

Having based its interpretation on a "permissible construction of the statute," the Commission also discharged its responsibility to "articulate[] a satisfactory explanation" for its choice of definition within the statutory range. *Mozilla Corp. v. FCC*, 940 F.3d 1, 49 (D.C. Cir. 2019) (internal citations omitted). The Commission reasonably concluded that "all equipment or services that include or use electronic components can be reasonably considered essential," and that this "bright-line rule" would "ease regulatory compliance and administrability." 2020 order ¶ 52. The Commission also reasonably rejected arguments that this definition was "unduly broad," because as the Commission noted, not all "essential" equipment would be placed on the Covered List; rather, only equipment that separately met criteria for posing a national-security threat would be deemed "covered." *Id.* ¶ 54.

Petitioners also err in arguing that end-user devices, like video cameras and recorders, cannot qualify as covered "communications equipment" because they are merely incidental to the network. Indeed, the text and legislative history of the NDAA reveal Congress's concern that end-user equipment could pose a threat to the security of American broadband networks. Petitioners' assertion (at 28) that their equipment "does not raise concerns" "of the sort Congress intended to address"

could not be further from the truth. Chinese company ZTE, for example, is a "cell phone maker"—yet Congress chose to include it in Section 889 because its manufacture of phones, servers, and "cameras," Senator Marco Rubio observed, "is a big danger." 164 Cong. Rec. S5,541-01 (daily ed. Aug. 1, 2018). Senator Sherrod Brown similarly emphasized that because ZTE "make[s] cheap smartphones," "a company that knowingly breaks U.S. laws could have control over information people have on their phones." 164 Cong. Rec. S3,285-02 (daily ed. June 7, 2018). Given Congress Members' concern about ZTE cell phones, Petitioners' argument that Congress intended to exclude video-surveillance equipment from the term "communications equipment or service" is meritless.

Nor do Petitioners gain mileage by arguing (at 30–31) that their equipment is not "used in" broadband networks. The Commission explained in the Order under identifying video-surveillance review by equipment communications equipment under the Secure Networks Act, by reference to section 889(f)(3)," "Congress intended to capture ... video surveillance equipment as 'covered equipment,' even if it is not core network equipment," because that equipment "is used (and indeed required) in the provision of a certain type of advanced communication service, i.e., video surveillance services." Order 7608. The Commission reasonably relied on this Congressional determination, as well as the reality that Hikvision's and Dahua's equipment "can be interconnected" to networks,

# B. The FCC's Decision To Accord Dispositive Weight To Congress's National-Security Determination Was Reasonable.

The Commission also reasonably concluded that it did not need to conduct an independent inquiry into the technical capabilities of equipment that Congress identified under the NDAA as posing a national-security risk before placing that equipment on the Covered List, given Section 1601(b)'s plain language, which provides that the FCC shall place on the Covered List any equipment that:

- (1) ...based exclusively on the determinations described in paragraphs (1) through (4) of subsection (c) ... poses an unacceptable risk to the national security of the United States ...; and
- (2) is capable of—
- (A) routing or redirecting user data traffic or permitting visibility into any user data ...;
- (B) causing the network of a provider of advanced communications service to be disrupted remotely; or
- (C) otherwise posing an unacceptable risk to the national security of the United States.

47 U.S.C. § 1601(b). One exclusive determination described in subsection (c), as relevant here, is that the equipment is "covered telecommunications equipment or services" under the NDAA. *Id.* § 1601(c)(3).

In the NDAA, Congress determined that Petitioners' equipment is "covered telecommunications equipment or services," and thus "poses an unacceptable risk to the national security of the United States." And because Congress determined that Petitioners' equipment threatens national security, the FCC unsurprisingly concluded that Petitioners' equipment "is capable of ... posing an unacceptable risk to the national security" under Section 1601(b)(2). Section 1601(b) therefore required the FCC to place Petitioners' equipment on the Covered List.

Petitioners resist that conclusion by proposing a judicial rewrite of the statutory language. Although Petitioners' brief never advances an argument that their equipment does not actually "pos[e] an unacceptable risk to the national security of the United States," *id.* § 1601(b)(2)(C)—nor do they contest that Congress found exactly that—they assert that Section 1602(b)(2) nevertheless is not satisfied because posing an unacceptable risk to national security is (in their view) not enough. According to Petitioners (at 36), Section 1602(b)(2)(C) requires a specific kind of unacceptable national-security risk, one "related to a device's ability to interact harmfully with a network," and Congress left those words for the judiciary to fill in. But "[i]t is not for the Court to rewrite the statute so that it covers only what the Court thinks is necessary to achieve what the Court thinks Congress really intended." *Lewis v. City of Chicago*, 560 U.S. 205, 215 (2010) (cleaned up).

Petitioners cite the noscitur a sociis and ejusdem generis canons (at 36) to defend their blue penciling, but those canons cannot carry nearly the weight Petitioners demand. Petitioners argue (at 36) that because Section 1601(b)(2)'s first two criteria "are specific to a device's ability to cause some harm through interaction with a network," the third criterion—that equipment "pos[e] an unacceptable risk to national security"—is also limited to network-interaction harm. That is wrong.

As an initial matter, Section 1601(b)(2) is a poor candidate for the noscitur and ejusdem canons because—as Petitioners concede—both doctrines apply when the "term" in question "is directly preceded by a list of terms." Overdevest Nurseries, L.P. v. Walsh, 2 F.4th 977, 983 (D.C. Cir. 2021); see also Pet. Br. 36 (same). A paradigmatic application of the *ejusdem* canon, for example, is the phrase "dogs, cats, horses, cattle, and other animals." Antonin Scalia & Bryan A. Garner, Reading Law 199 (2012). Section 1601(b)(2), of course, is not a list, and it contains detailed phrases, not terms. Additionally, that the criteria are "made separate and distinct from one another by Congress' use of the disjunctive" is another indicator that the ejusdem canon does not apply. Garcia v. United States, 469 U.S. 70, 75 (1984).

The Supreme Court has cautioned, moreover, that courts must not place more weight on these canons than they can bear. The Court "has often noted" that ejusdem "is only an instrumentality for ascertaining the correct meaning of words when there is uncertainty." Harrison v. PPG Indus., Inc., 446 U.S. 578, 588 (1980); see also,

e.g., Ali v. Fed. Bureau of Prisons, 552 U.S. 214, 227 (2008) ("[W]e do not woodenly apply limiting principles every time Congress includes a specific example along with a general phrase"); Brett M. Kavanaugh, Fixing Statutory Interpretation, 129 Harv. L. Rev. 2118, 2160 (2016) ("[W]e have to be wary of adding implicit limitations to statutes that the statutes' drafters did not see fit to add."). Absent uncertainty, courts must interpret statutory language "to mean exactly what it says." Harrison, 446 U.S. at 589; Garcia, 469 U.S. at 75 (rejecting ejusdem argument for lack of "ambiguity in the plain meaning of the words"); United States v. Turkette, 452 U.S. 576, 581 (1981) (ejusdem "comes into play only when there is some uncertainty as to the meaning of a particular clause in a statute"). Petitioners do not assert that Section 1601(b)(2) is ambiguous, and the fact that they do not like its "literal" import is no basis for judicial rewrite. Harrison, 446 U.S. at 589 n.6. Moreover, the Supreme Court has directly rejected Petitioners' argument (at 35–36, 36-37) that the natural reading of a broad category should be rejected because it allegedly "swallows" prior-listed categories. See Ali, 552 U.S. at 227 (explaining that *Harrison* "reject[ed] an argument that *ejusdem generis* must apply when a broad interpretation of the clause could render the specific enumerations unnecessary"). Because Congress used an "unmodified, all-encompassing phrase" that contains no ambiguity, the statute must be read "to mean what it literally says." *Id.* at 227–28.

Filed: 08/07/2023 Page 42 of 53

Petitioners' reading also fails because it violates the presumption that statutory words "have the same meaning in all subsections of the same statute." Morrison-Knudsen Constr. Co. v. DOL, 461 U.S. 624, 633 (1983). Section 1601 uses the very phrase at issue—"an unacceptable risk to the national security of the United States or the security and safety of United States persons"—in the preceding paragraph, and that paragraph undisputedly does not carry the network-interaction limitation Petitioners seek to impose on Section 1601(b)(2). Indeed, Petitioners concede (at 37 n.8) that on their reading this phrase "carries different meanings in paragraph (b)(1) and subparagraph (b)(2)(C)."

Petitioners argue (at 37 n.8) that the consistent-usage canon "yields to context" in this instance, but their argument fails because they again need ambiguity that does not exist. In the case they cite, the Supreme Court held that a reference in the America Invents Act to a "person" does not include the government even though the patent statutes sometimes use that word as government inclusive. Return Mail, Inc. v. United States Postal Serv., 139 S. Ct. 1853, 1863 (2019). The Court emphasized that the patent statutes "refer to 'person[s]' in at least 18 different places, and there is no clear trend: Sometimes 'person' plainly includes the Government, sometimes it plainly excludes the Government." Id.

But whereas the patent statutes contain undisputed uses of the word "person" carrying both relevant meanings, here Petitioners cannot point to a single use of the

contested phrase that undisputedly carries their preferred meaning. Moreover, Section 1601(b) uses not an abstract single word like "person" but rather repeats a twenty-word phrase in identical language. Compare 47 U.S.C. § 1601(b)(1) ("an unacceptable risk to the national security of the United States or the security and safety of United States persons"); with id. § 1601(b)(2)(C) ("an unacceptable risk to the national security of the United States or the security and safety of United States persons"). This repetition can only be understood as deliberate—if Congress meant to convey a different idea in the second iteration of a twenty-word phrase, it easily could have changed something to indicate as much. And Section 1601(b) uses the unacceptable-risk phrase in back-to-back provisions of a single subsection whose provisions do not have grab-bag objectives but rather share the subject matter of the creation of the Covered List. Compare Returned Mail, 139 S. Ct. at 1863 (statutory term "is used throughout the statute" and "takes on 'distinct characters' in distinct statutory provisions"); see also Scalia & Garner, Reading Law 173 (consistent-usage canon is particularly forceful when usages were "enacted at the same time" and "dealt with the same subject").

When "unacceptable risk to the national security" is read to mean what it says, it is apparent that the FCC reasonably determined that Petitioners' equipment is *capable* of posing such an unacceptable risk because Congress determined that Petitioners' equipment *in fact does* pose such a risk. Incredibly, Petitioners argue (at

Filed: 08/07/2023 Page 44 of 53

38–39) that in determining whether their equipment "pos[es] an unacceptable risk to the national security," Section 1601(b)(2)(C), the FCC was required to disregard the views of the United States Congress. But Section 1601(b)(2) says nothing of the sort. While innumerable statutes require an agency to bring its independent judgment to bear on a particular question, e.g., 20 U.S.C. § 1098bb(a)(1) (Secretary of Education may waive or modify certain student-aid provisions "as the Secretary deems necessary" in connection with a military operation or national emergency), Section 1601(b)(2) is not one of them. Section 1601(b)(2) simply says that equipment shall be placed on the Covered List if the equipment "is" capable of posing an unacceptable risk to national security. It was eminently reasonable for the FCC to determine that equipment Congress deems threatening to national security is in fact threatening to national security.

Petitioners argue (at 35) that the FCC's reading "would render an entire subparagraph [i.e., Section 1601(b)(2)] meaningless," but that is not true—under the FCC's reading, Section 1601(b)(2) will sometimes operate independently of Section 1601(b)(1). See Respondent Br. 50. Even if Section 1601(b)(2) does not have "heavy work ... to perform," "a job is a job, and enough to bar the rule against redundancy from disqualifying an otherwise sensible reading." Polselli v. IRS, 143 S. Ct. 1231, 1239 (2023); see also Nielson v. Preap, 139 S. Ct. 954, 969 (2019) (a clause that "still has work to do" is not superfluous). And most importantly, the surplusage

canon cannot trump the text's plain meaning. See, e.g., Conn. Nat. Bank v. Germain, 503 U.S. 249, 253-54 (1992) ("in interpreting a statute a court should always turn first to one, cardinal canon before all others," i.e., plain meaning); Lamie v. U.S. Tr., 540 U.S. 526, 536 (2004) (plain meaning trumps surplusage canon).

Finally, Petitioners' assertion (at 38–39, 40) that their equipment is not "capable of ... routing or redirecting user data traffic or permitting visibility into any user data" is inconsistent with the record. A video-surveillance system can be configured to permit a party to access content that the system "transmits or otherwise handles," 47 U.S.C. § 1601(b)(2)(A), even if it is a "peripheral, non-network device[]," Pet. Br. 7; see also Order 7608. Petitioners cannot avoid the Covered List or circumvent Section 889 simply because an end user needs to take additional steps to connect an insecure device to a network, precisely as the device's manufacturer intended. Regardless of the entity enabling interconnection of Petitioners' cameras, their equipment raises the security risks that concerned Congress when it enacted the SNA and Section 889.

Congress's concerns are illustrated by Motorola's experience with Hytera, one of the companies identified in Section 889. Hytera engaged in rampant theft of Motorola's intellectual property, which resulted in an Illinois jury verdict fully in Motorola's favor, a judgment in excess of \$631 million after finding that Hytera willfully and maliciously misappropriated Motorola's trade secrets and infringed its

copyright source code, and other relief. See Motorola Sols., Inc. v. Hytera Commc'ns Corp., No. 1:17-cv-1973, 2021 WL 3076780, at \*2-3 (N.D. Ill. Mar. 10, 2021). The judge wrote that Hytera's trade-secret theft "was not only willful and malicious, but egregious," because it "stole the entirety of Motorola's highly confidential DMR source code and thousands of confidential documents ... to develop competing products." Id. Over the course of the litigation, Motorola uncovered evidence demonstrating that Hytera stole over ten thousand confidential documents and millions of lines of source code. Hytera then compounded its wrongdoing through repeated efforts to illegally conceal its theft—including "rewriting code to look different from Motorola's and ... taking extensive measures to destroy evidence or to ensure that no such evidence existed." Id.

More generally, as the Commission discussed at length in its 2020 order upheld in *Huawei*, "companies' ties to the Chinese government," along with "Chinese laws obligating them to cooperate with any request by the Chinese government to use or access their systems," "pose a threat to the security of communications networks and the communications supply chain." 85 Fed. Reg. 230-01 ¶ 5, 2020 WL 30573 (Jan. 3, 2020). And Covered List equipment producers undeniably have ties to China—Hikvision, for example, has acknowledged that its largest shareholder is a "Chinese state-owned enterprise." Comments of Hikvision USA, Inc. at 15, ET Docket No. 21-232, EA Docket No. 21-233 (filed Sept. 20,

2021). The judiciary should not second guess the political branches' shared view of the threat Petitioners' equipment poses.

## III. The FCC Reasonably Construed The Scope Of "Critical Infrastructure"

Finally, Petitioners fail to raise any legal infirmity in how the Commission proposed to construe the scope of "critical infrastructure" to determine what types of equipment would be included on the Covered List.

Petitioners manage to discuss the FCC's "interpretation of 'critical infrastructure" (capitalization omitted) for seven paragraphs before citing any order of the FCC, and in total their eight-page discussion of the issue (at 50–58) cites the FCC only twice. Unsurprisingly, then, Petitioners misapprehend what the Order actually does. It does not, contrary to Petitioners' claim (at 50), proclaim that "everything is 'critical," or that anything connected to a sector connected to national security is necessarily critical. Rather, it merely states that the FCC defines "critical infrastructure" by reference to how that term is defined elsewhere in federal law and indicates that further guidance from the FCC, in coordination with other expert national-security agencies, will be forthcoming. Petitioners do not argue that their ability to market or sell any piece of equipment has been limited by the FCC's definition of "critical infrastructure," which is an acknowledgement that their petition is meritless and premature.

In the Order, the FCC stated that it was prohibiting as covered equipment the authorization of any of Petitioners' video-surveillance equipment "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." Order 7614 (quoting Section 889(f)(3)(B)). With respect to "critical infrastructure," the FCC stated that it was adopting "the meaning provided in section 1016(e) of the USA Patriot Act of 2001, namely, 'systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Id. at 7615. The FCC further noted that Presidential Policy Directive 21 "identifies sixteen critical infrastructure sectors" and that in publishing a set of 55 National Critical Functions to guide national risk management efforts, CISA defined "critical infrastructure" similar to its USA Patriot Act definition. Id. The FCC found that for the purposes of the Order, any systems or assets connected to the sixteen critical infrastructure sectors identified in Presidential Policy Directive 21 or the 55 National Critical Functions identified by CISA "could" be considered critical infrastructure. Id.

The FCC did not determine that any specific facility is "critical infrastructure," nor did it determine that any piece of equipment surveils critical infrastructure. Rather, the Order establishes parameters for what critical

Filed: 08/07/2023 Page 49 of 53

infrastructure is and states that further determinations about specific equipment will be forthcoming. Specifically, the Order creates a process whereby Petitioners can obtain approval for their equipment so long as they demonstrate that it will not be used for any prohibited purpose. See id. at 7609 ("[T]hese entities must each seek and obtain Commission approval for its respective plan that will ensure that such equipment will not be marketed or sold '[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.""). And the Order instructs the FCC Bureaus to "develop further clarifications to inform applicants for equipment authorization ... with more specificity and detail," and to "coordinate as necessary with [our] federal partners, such as but not limited to the Department of Justice, Department of Commerce, Department of Homeland Security, and Federal Bureau Investigation." Id. at 7615.

But the FCC has not yet determined how the term will be applied to specific situations. When the equipment-approval process plays out, disappointed applicants will have an opportunity to seek review. Until then, Petitioners' apparent challenge to specific applications of the critical-infrastructure definition is not ripe for review. Cf. Huawei, 2 F.4th at 435 ("Huawei fails to show the initial designation is the 'consummation' of the FCC's decisional process.").

And Petitioners' challenge is meritless in any event. Because "the FCC's judgments ... are informed by agencies with much more expertise than the FCC on these matters," the authority it exercises under the Order "closely resembles the kind of national security authority it has exercised for decades—limited, communications-focused judgment informed by expert agencies and deferential to their views." Id. at 443. And it is simply not true that under the Order "all infrastructure is critical, including laundromats and used car lots." Pet. Br. 50. The FCC has not taken a position on the precise scope of the critical-infrastructure inquiry—rather, it has outlined parameters for when infrastructure "could" be considered critical. Order 7615. Because those parameters simply reflect the definitions of critical infrastructure used elsewhere in federal law and adopted by other federal agencies, the FCC's approach to the critical-infrastructure inquiry was reasonable.

#### **CONCLUSION**

This Court should dismiss the petitions for review.

Respectfully submitted,

/s/ Thomas M. Johnson, Jr.

Thomas M. Johnson, Jr. *Counsel of Record*Bennett L. Ross
Michael J. Showalter

### WILEY REIN LLP

2050 M Street NW Washington, DC 20036 (202) 719-7000 tmjohnson@wiley.law

Counsel for Motorola Solutions, Inc.

Filed: 08/07/2023

August 7, 2023

#### **CERTIFICATE OF COMPLIANCE**

This brief complies with the type-volume limitations of Federal Rule of Appellate Procedure 32(a)(7)(B) because it contains 9029 words, excluding the parts of the brief exempted by Rule 32(f) and D.C. Circuit Rule 32(e)(1). This brief complies with the typeface requirements of Rule 32(a)(5) and the type style requirements of Rule 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in Times New Roman and 14-point font.

/s/ Thomas M. Johnson, Jr.

Thomas M. Johnson, Jr.

August 7, 2023

## **CERTIFICATE OF SERVICE**

I hereby certify that on August 7, 2023, the foregoing brief was filed via CM/ECF. Service was accomplished on all parties or their counsel of record via CM/ECF.

/s/ Thomas M. Johnson, Jr.

Thomas M. Johnson, Jr.

August 7, 2023